RECEIVED
CENTRAL FAX CENTER

NOV 15 2004

MOTOROLA

Intellectual Property Section
Law Department

FAX COVER SHEET

DATE: NOVEMBER 15, 2004

TO: EXAMINER SHIN (ADDRESSEE'S NAME) — 703-305-0711 (EXTENSION)
ART UNIT 2143 (LOCATION) — 703-872-9306 (FAX NUMBER)

FROM: MATTHEW C. LOPPNOW (SENDER'S NAME) — (847) 523-2585 (EXTENSION)

RE: APPLICATION NO.: 09/575,749

TOTAL NUMBER OF PAGE(S) 18 (INCLUDING THIS PAGE)

NOTICE: This facsimile transmission may contain information that is confidential, privileged or exempt from disclosure under applicable law. It is intended only for the person(s) to whom it is addressed. Unauthorized use, disclosure, copying or distribution may expose you to legal liability. If you have received this transmission in error, please immediately notify us by telephone (collect) to arrange for return of the documents received and any copies made. Thank you.

Personal Communications Sector
600 North U.S. Highway 45, AN 475
Libertyville, IL 60048
Phone: (847) 523-2322 Facsimile: (847) 523-2350

BEST AVAILABLE COPY

RECEIVED
CENTRAL FAX CENTER

NOV 15 2004

I hereby certify that this correspondence is being facsimile transmitted to the U.S. Patent and Trademark Office (Fax No. 703-872-9306) on the date indicated below.

Signature _____ Date November 15, 2004
Matthew C. Loppnow

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Alberth et al.	EXAMINER: Shin, K.
SERIAL NO.: 09/575,749	GROUP: 2143
FILED: May 22, 2000	CASE NO.: CS10614
ENTITLED: SMART CARD WITH BACK UP	

Motorola, Inc.
Intellectual Property Department
600 North U.S. Highway 45
Libertyville, IL 60048

APPEAL BRIEF UNDER 37 C.F.R. § 1.192(c)

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Further to the Notice of Appeal filed on October 18, 2004, Applicant submits the present Appeal Brief.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is, Motorola, Inc.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-19 are pending. Claims 1-19 are rejected and are the subject of the present appeal.

IV. STATUS OF AMENDMENTS

No amendments were filed subsequent to final rejection.

V. SUMMARY OF INVENTION

The inventions are drawn generally to a method and apparatus for securely storing data in a personal data security device commonly known as a smart card (page 1, lines 4-6, Fig. 1, element 100). An additional layer of security is provided to the smart card (100) in the form of a second part (112), such as an enabling key, of the smart card, which when coupled to a first part (102) of the smart card, enables the processor on the smart card to access and change stored information. If the second part (112) is not accessible to the first part (102), the smart card function remains disabled (page 2, lines 10-14 and page 5, lines 19-22).

VI. ISSUES

Whether claims 1-19 are allowable under 35 U.S.C. § 102 over Storck et al. (U.S. Patent No. 5,434,395).

PAGE 4/18 * RCVD AT 11/15/2004 6:20:22 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:18475232350 * DURATION (mm-ss):04-16

VII. GROUPING OF CLAIMS

Claims 1, and 14 do not stand or fall with claim 8 or claim 18 regarding the rejection thereof under 35 U.S.C. § 102.

VIII. ARGUMENT

Claim Limitations At Issue

The limitations at issue in claims 1, 8, 14, and 18 are italicized below:

1. A personal data storage apparatus comprised of:
   a. a first personal data storage device including a memory device storing:
      i. a first set of user data;
      ii. a first encryption key for encrypting at least part of said first set of user data;
   b. *a first interface circuit coupled to said memory device granting conditional access to a third device to data therein using an appropriate data exchange protocol between the first personal data storage device and the third device only when a second personal data storage device is operatively coupled to said first personal data storage device*; and
   c. a second interface circuit coupled to said memory device and providing communications access to the second personal data storage device.

8. A personal data storage apparatus comprised of:
   a. a first personal data storage device comprising:
      i. a first memory device storing:
         1. a first set of user data;
         2. a first encryption key for encrypting at least part said first set of user data;

ii. *a first interface circuit coupled to said memory device granting conditional access to data therein using a predetermined protocol and only when a second personal data storage device is operatively coupled to said first personal data storage device;*

iii. a second interface circuit coupled to said memory device and providing access to a second personal data storage device;

b. a second personal data storage device coupled to said first personal data storage device and being comprised of:

i. a second memory device storing:

1. *a substantially duplicate copy of said first set of user data;*

c. a second encryption key for encrypting at least part said first set of user data;

ii. *a second interface circuit coupled to said memory device granting conditional access to data therein using a predetermined protocol and only when said second personal data storage device is operatively coupled to said first personal data storage device;*

whereby user data in either said first or second personal data storage device is accessible and usable only when said first and second personal data storage devices are in communication with each other.

14. A method of securing access to data stored in a personal data storage device comprised of the steps of:

a. storing personal data in first and second data storage devices that are capable of being operably coupled to each other;

b. encrypting said personal data in a first data storage device using a first encryption key and encrypting it in said second data storage device using a second encryption key;

c. *granting access to a third device to said personal data in either said first data storage device or said second data storage device only when said first and second data storage devices are operatively coupled together.*

18. A method of securing access to data stored in a personal data storage device comprised of the steps of:

a. storing personal data in a smart card and an enabling key device that are capable of being operably coupled to each other;

b. encrypting said personal data in the smart card using a first encryption key and encrypting said personal data in the enabling key device using a second encryption key; and

c. *prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together.*

Examiner's Allegation

Claims 1-19 stand rejected under 35 U.S.C. § 102 over Storck et al. (U.S. Patent No. 5,434,395).

Applicants' Argument

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference" (MPEP §2131, citing Verdegaal Bros. v. Union Oil Co. of California, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

Applicants assert that Storck et al. does not disclose or suggest granting access to a third device to said personal data therein only when a second data storage device is operatively coupled to a first data storage device, as recited in independent claim 1. Storck et al. also does not disclose granting access to a third device to said personal data in either said first data storage device or said second data storage device only when said first and second data storage devices are operatively coupled together, as recited in independent claim 14.

Applicants also assert Storck et al. does not disclose prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together, as recited in independent claim 18.

Applicants also assert that Storck et al. does not disclose or suggest second personal data storage device storing a substantially duplicate copy of a first set of user data stored in a

PAGE 7/18 * RCVD AT 11/15/2004 6:20:22 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:18475232350 * DURATION (mm-ss):04-16

first personal data storage device, whereby user data in either said first or second personal data storage device is accessible and usable only when said first and second personal data storage devices are in communication with each other as recited in independent claim 8.

Storck et al. uses an interfacing circuit that controls data transfer between one data carrier and another data carrier when the data carriers are identified as compatible(Abstract). There is no disclosure of granting access to said personal data in either said first data storage device or said second data storage device to a third device only when said first and second data storage devices are operatively coupled together and there is no disclosure of prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together and such is not asserted by the original Office Action.

Storck et al. does not disclose that data in either said first or second personal data storage device is accessible and usable only when said first and second personal data storage devices are in communication with each other. In particular, Storck et al. discloses controlling data transfer between data carriers when they are identified as compatible with each other. There is no disclosure that the data is not accessible and usable when two specific carriers are not in communication with each other. More particularly, Storck et al. expressly discloses that transactions can be carried out between several microcircuit cards (col. 4, lines 31-34). Storck et al. does not disclose that data in either said first or second personal data storage device is accessible and usable only when said first and second personal data storage devices are in communication with each other or prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together.

Furthermore, Storck et al. does not disclose that each carrier having a duplicate copy of data where data is accessible and usable only when the carriers are in communication with each other, as recited in independent claim 8. In particular, Storck et al. is directed to an interfacing circuit for controlling data transfer between the two carriers, which is the opposite of each carrier having a duplicate copy of data where data is accessible and usable only when the carriers are in communication with each other. In particular, if each carrier in Storck et al. had a duplicate copy of data, it would be unnecessary to use an interfacing circuit to control data transfer between the carriers. Thus, Storck et al. does not disclose that each carrier

having a duplicate copy of data where data is accessible and usable only when the carriers are in communication with each other, as recited in independent claim 8.

In the Response to Amendment section, the final Office Action alleges Storck et al. discloses, at col. 12, lines 45-48, "The authorization level is divided between two personal data storage devices such that data transfer to a third device is possible only when a first and a second personal data storage device are coupled together or used simultaneously, e.g. operating at the same time." Applicants disagree. In particular, col. 12, lines 45-48 do not disclose data transfer to a third device is possible only when a first and a second personal data storage device are coupled together." More particularly, the cited passage only discloses it is "possible to divide up an authorization level between two or several slave cards which will then need to be used in a complementary manner or simultaneously." However, this not the disclosure of two or several slave cards being coupled together. In particular, "simultaneously" only describes slave cards being used at the same time. It is not the disclosure of a two data storage devices being operatively coupled together. Using two devices in a complementary manner is not the disclosure of a two data storage devices being operatively coupled together. For example, each device may be used in a complementary manner or simultaneously by each being separately coupled to the third device without being operatively coupled to each other. In particular, Fig. 4 expressly illustrates numerous slots or fields 43 and Fig. 5 also expressly illustrates numerous slots or fields 49. Thus, cards are used simultaneously by coupling each to the fields of the device 42 or 46, but not to each other. To the contrary, applicants are positively claiming only granting access to a third device only when two devices are operatively coupled together and such is not disclosed by Storck et al.

Furthermore, Storck et al. expressly discloses that a user can carry out any data processing operation in combination with one or several microcircuit cards (col. 13, lines 40-43). This is the exact opposite of the claimed granting access to a third device to data in a memory of a first device only when a second personal data storage device is operatively coupled to the first device or prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together. In particular, this expressly illustrates that access is granted to a third device, the device in Fig. 4, to data in a first device, such as one microcircuit card, without the presence of a second device, a second microcircuit card. This illustrates how Storck et al. clearly does not disclose

PAGE 9/18 * RCVD AT 11/15/2004 6:20:22 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:18475232350 * DURATION (mm-ss):04-16

granting access to a third device to data in a memory of a first device only when a second personal data storage device is operatively coupled to the first device.

Thus, Storck et al. does not disclose or suggest granting access to a third device to said personal data therein only when a second data storage device is operatively coupled to a first data storage device, as recited in independent claim 1. Storck et al. also does not disclose granting access to a third device to said personal data in either said first data storage device or said second data storage device only when said first and second data storage devices are operatively coupled together, as recited in independent claim 14. Storck et al. also does not disclose prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together, as recited in independent claim 18.

In the Response to Amendment section, the final Office Action also alleges Storck et al. discloses, at col. 4, lines 52-58, that data is not accessible when two specific carrier, personal data storage devices, are not in communication with each other. Unfortunately, the Office Action mischaracterizes the referenced passage. In particular, the referenced passage expressly states, "The invention further has the advantage of enabling a person owning or in possession of a card to read the data contained therein. Obviously, this can mean that such information cannot be read until the owner has entered a personal identification number code. Any other operation carried out by the use of the card may necessitate the owner introducing said code." However, this is the exact opposite of what the Office Action is alleging. In particular, the cited passage clearly illustrates that data in a card can be read without the presence of another device. More particularly, the presence of another device is not required because the data in a card can be read by merely entering a personal identification number. This is completely contradictory to the claimed invention, which positively recites data in either the first or second personal data storage device is accessible and usable only when the first and second personal data storage devices are in communication with each other. This is also contradictory to claim 18, which positively recites prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together. In fact that Office Action expressly admits that data cannot be read without authorization whether two specific carriers are in communication or not. This implies that data can be read with authorization when two carriers are not in communication,

which is not the case of data being accessible and usable only when two devices are in communication with each other.

Thus, Storck et al. does not disclose or suggest granting access to a third device to said personal data therein only when a second data storage device is operatively coupled to a first data storage device, as recited in independent claim 1. Storck et al. also does not disclose granting access to a third device to said personal data in either said first data storage device or said second data storage device only when said first and second data storage devices are operatively coupled together, as recited in independent claim 14.

Also, Storck et al. does not disclose prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together, as recited in independent claim 18.

Additionally, Storck et al. does not disclose or suggest second personal data storage device storing a substantially duplicate copy of a first set of user data stored in a first personal data storage device, whereby user data in either said first or second personal data storage device is accessible and usable only when said first and second personal data storage devices are in communication with each other as recited in independent claim 8.

Therefore, Applicants respectfully submit that independent claims 1, 8, 14, and 18 define patentable subject matter. The remaining claims are either not rejected or depend from the independent claims and therefore also define patentable subject matter. Accordingly, Applicants respectfully request the withdrawal of the rejection under 35 U.S.C. § 102.

Kindly reverse and vacate the rejection of claims 1, 8, 14, and 18 under 35 U.S.C. § 102, with instructions for the Examiner to allow claims 1-19.

CONCLUSION

In view of the discussion above, the claims of the present application are in condition for allowance. Kindly withdraw any rejections and objections and allow this application to issue as a United States Patent without further delay.

PAGE 11/18 * RCVD AT 11/15/2004 6:20:22 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:18475232350 * DURATION (mm-ss):04-16

The Commissioner is hereby authorized to deduct the amount of $340 for filing a brief in support of an appeal and any fees arising as a result of this Appeal Brief or any other communication from or to credit any overpayments to Deposit Account No. 50-2117.

Respectfully submitted,

Matthew C. Loppnow
Attorney for Applicant
Registration No. 45,314

Phone No. (847) 523-2585

Dated: November 15, 2004

Fax No. (847) 523-2350
Please send correspondence to:
Motorola, Inc.
Intellectual Property
600 North U.S. Highway 45
Libertyville, IL 60048

PAGE 12/18 * RCVD AT 11/15/2004 6:20:22 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:18475232350 * DURATION (mm-ss):04-16

IX. APPENDIX

1. (previously presented) A personal data storage apparatus comprised of:

a. a first personal data storage device including a memory device storing:

i. a first set of user data;

ii. a first encryption key for encrypting at least part of said first set of user data;

b. a first interface circuit coupled to said memory device granting conditional access to a third device to data therein using an appropriate data exchange protocol between the first personal data storage device and the third device only when a second personal data storage device is operatively coupled to said first personal data storage device; and

c. a second interface circuit coupled to said memory device and providing communications access to the second personal data storage device.

2. (original) The personal data storage apparatus of claim 1 further comprised of a processor, operatively coupled to said memory device and to said first and second interface circuits.

3. (original) The personal data storage apparatus of claim 1 wherein said second personal data storage device is operatively coupled to said first personal storage device using a mechanical coupling.

4. (original) The personal data storage apparatus of claim 3 wherein said mechanical coupling is a connector.

5. (original) The personal data storage apparatus of claim 1 wherein said second personal data storage device is operatively coupled to said first personal storage device using a wireless connection.

6. (original) The personal data storage apparatus of claim 5 wherein said wireless connection is a radio link.

7. (original) The personal data storage apparatus of claim 1, where an agent of the issuer of the personal data storage apparatus can reclaim the user data from a single part of the personal data storage apparatus.

8. (previously presented) A personal data storage apparatus comprised of:

a. a first personal data storage device comprising:

i. a first memory device storing:

1. a first set of user data;

2. a first encryption key for encrypting at least part said first set of user data;

ii. a first interface circuit coupled to said memory device granting conditional access to data therein using a predetermined protocol and only when a second personal data storage device is operatively coupled to said first personal data storage device;

iii. a second interface circuit coupled to said memory device and providing access to a second personal data storage device;

PAGE 14/18 * RCVD AT 11/15/2004 6:20:22 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:18475232350 * DURATION (mm-ss):04-16

b. a second personal data storage device coupled to said first personal data storage device and being comprised of:

i. a second memory device storing:

1. a substantially duplicate copy of said first set of user data;

c. a second encryption key for encrypting at least part said first set of user data;

ii. a second interface circuit coupled to said memory device granting conditional access to data therein using a predetermined protocol and only when said second personal data storage device is operatively coupled to said first personal data storage device;

whereby user data in either said first or second personal data storage device is accessible and usable only when said first and second personal data storage devices are in communication with each other.

9. (original) The personal data storage apparatus of claim 8 wherein said first personal data storage device is further comprised of a processor, operatively coupled to said first memory device and to said first and second interface circuits.

10. (original) The personal data storage apparatus of claim 9 wherein said second personal data storage device is operatively coupled to said first personal storage device using a mechanical connector.

11. (original) The personal data storage apparatus of claim 8 wherein said second personal data storage device is operatively coupled to said first personal storage device using a wireless connection.

12. (original) The personal data storage apparatus of claim 8 wherein said wireless connection is a radio link.

13. (original) The personal data storage apparatus of claim 8, where an agent of the issuer of the personal data storage apparatus can reclaim the user data from a single part of the personal data storage apparatus.

14. (previously presented) A method of securing access to data stored in a personal data storage device comprised of the steps of:

a. storing personal data in first and second data storage devices that are capable of being operably coupled to each other;

b. encrypting said personal data in a first data storage device using a first encryption key and encrypting it in said second data storage device using a second encryption key;

c. granting access to a third device to said personal data in either said first data storage device or said second data storage device only when said first and second data storage devices are operatively coupled together.

15. (previously presented) The method of claim 14 wherein said step of granting access to a third device to said personal data in either said first data storage device or said

PAGE 16/18 * RCVD AT 11/15/2004 6:20:22 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:18475232350 * DURATION (mm-ss):04-16

second data storage device only when said first and second personal data storage devices are operatively coupled together is comprised of the step of granting access when said first and second personal data storage devices are coupled together through at least one of either a wireless data link or a mechanical connector.

16. (original) The method of claim 14 wherein data stored in said first storage device can be recovered from data stored in said second storage device.

17. (original) The method of claim 14 wherein said first and second encryption keys are the same.

18. (previously presented) A method of securing access to data stored in a personal data storage device comprised of the steps of:

a. storing personal data in a smart card and an enabling key device that are capable of being operably coupled to each other;

b. encrypting said personal data in the smart card using a first encryption key and encrypting said personal data in the enabling key device using a second encryption key; and

c. prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together.

19. (previously presented) The method of claim 18, wherein said step of prohibiting a transaction between the smart card and another device unless the smart card and the enabling key device are operatively coupled together is comprised of the step of

prohibiting the transaction unless the smart card and the enabling key device are coupled together through at least one of either a wireless data link or a mechanical connector.

PAGE 18/18 * RCVD AT 11/15/2004 6:20:22 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:18475232350 * DURATION (mm-ss):04-16

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.